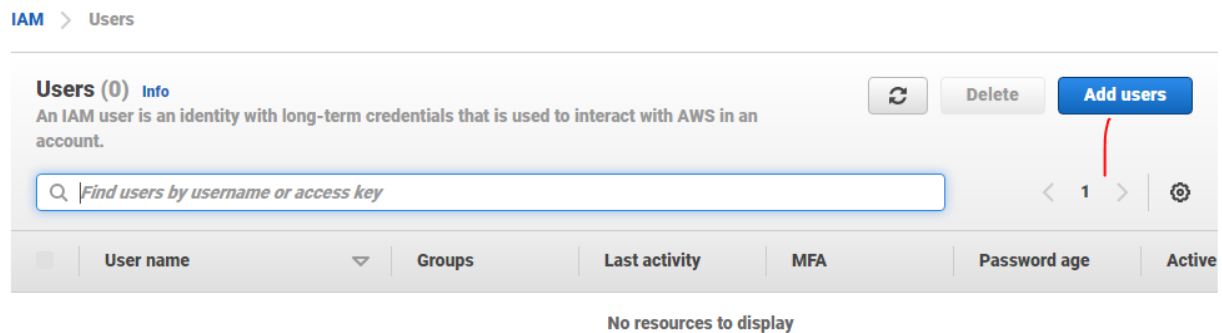


Lets upgrade –Day -1 Assignment

```
"Untitled - Notepad
File Edit Format View Help

Project 1
Working with IAM
Create 3 Users
Create one group
Set user permissions
Set a unique group permission
Login as the IAM user
Show the the user permission and the group permissions are applied
Check which policy gives access to IAM.
```

Steps-1 creating 3 -IAM users- given below--



Add user

- 1
- 2
- 3
- 4
- 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

Priya

Radhika

Anuradha

+

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

☒

Programmatic access

Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☒

AWS Management Console access

Enables a password that allows users to sign-in to the AWS Management Console.

Console password*

☐

Autogenerated password

☒

Custom password

Z

Add user

- 1
- 2
- 3
- 4
- 5

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

User details

User names	Priya, Radhika, and Anuradha
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary


The following policies will be attached to the users shown above.


Type	Name
Managed policy	AmazonEC2FullAccess


Add user

1 2 3 4 5

Set permissions









 Add users to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy

Filter policies Showing 25 results

	Policy name	Type	Used as
<input type="checkbox"/>	 AmazonEC2ContainerRegistryFullAccess	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerRegistryPowerUser	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerRegistryReadOnly	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerServiceEventsRole	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerServiceforEC2Role	AWS managed	None
<input type="checkbox"/>	 AmazonEC2ContainerServiceRole	AWS managed	None
<input checked="" type="checkbox"/>	 AmazonEC2FullAccess	AWS managed	None

Cancel Previous Next: Tags



Sign in as IAM user

Account ID (12 digits) or account alias

543509858019

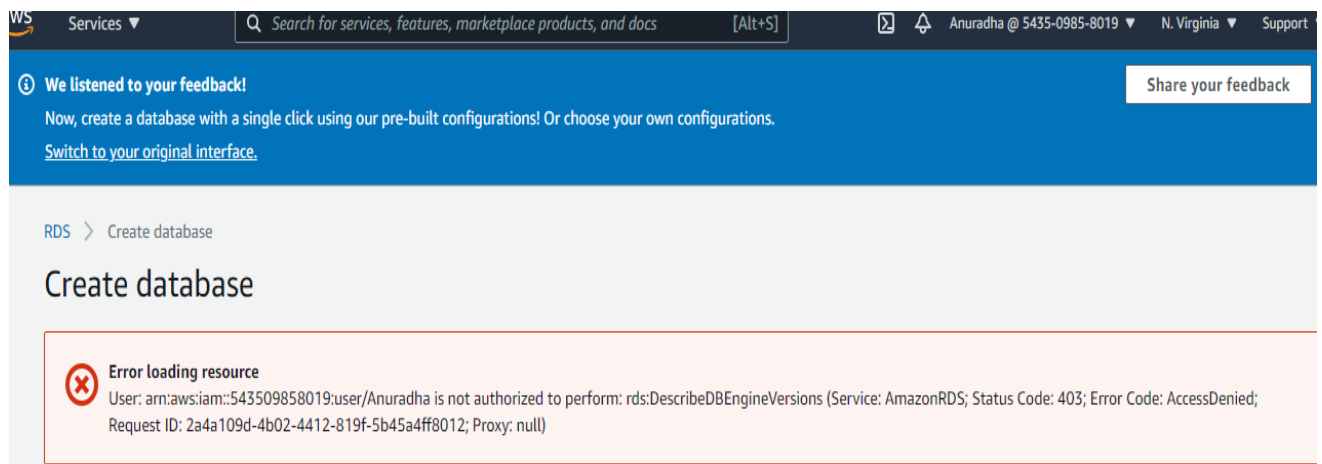
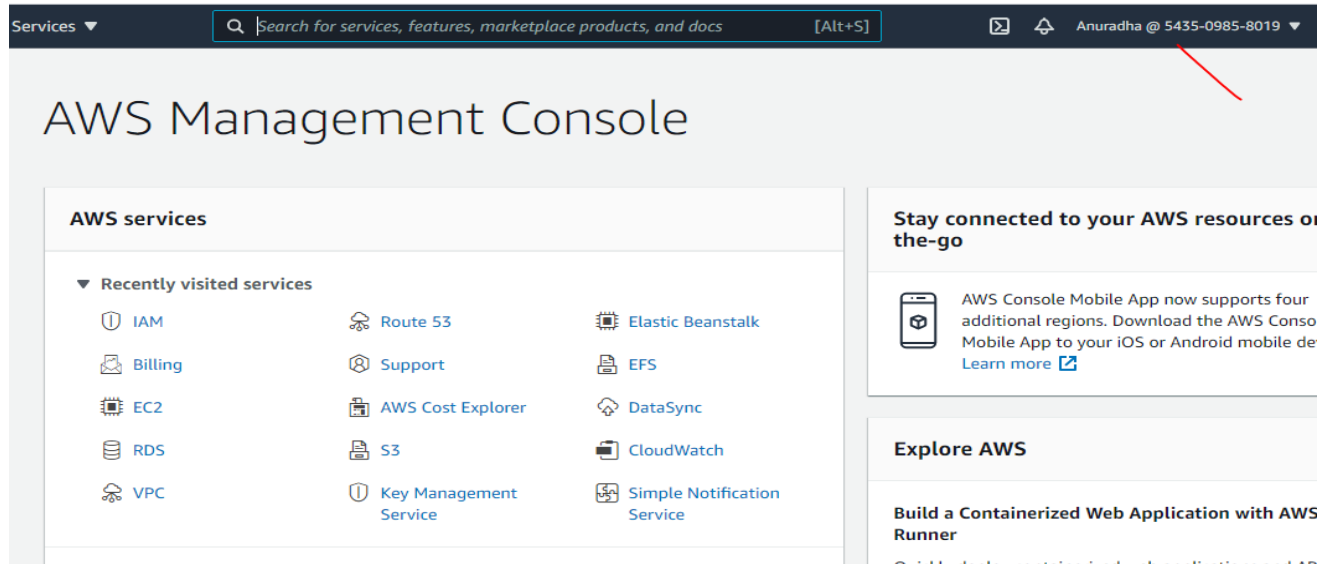
IAM user name

Anuradha

Password

Only EC2 permission is been given to the user Anuradha which is accessible.

Whereas other services are not permissible.



Here the user anuradha is not having permission to RDS domain to create database.

Now creating a group and give the permission. As follows

[IAM](#) > [User groups](#)

User groups (0) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

☐

Group name

▼

☐

Users

▼

☐

Permissions

▼

☐

Creation time

▼

No resources to display

✓ Solution-architect user group created.

[View group](#)

[IAM](#) > [User groups](#)

User groups (1) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

☐

Group name

▼

☐

Users

▼

☐

Permissions

▼

☐

Creation time

▼

☐

[Solution-architect](#)

2

✓ Defined

Now

Summary

[Edit](#)

User group name	Creation time	ARN
Solution-architect	August 02, 2021, 00:42 (UTC+05:30)	arn:aws:iam::543509858019:group/Solution-architect

[Users](#) | [Permissions](#) | [Access advisor](#)

Users in this group (2) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☐

User name [↗](#)

▼

☐

Groups

▼

☐

Last activity

▼

☐

Creation time

▼

☐

[Priya](#)

1

None

31 minutes ago

☐

[Radhika](#)

1

None

31 minutes ago

Solution-architect

[Delete](#)

Summary

[Edit](#)

User group name Solution-architect	Creation time August 02, 2021, 00:42 (UTC+05:30)	ARN arn:aws:iam::543509858019:group/Solution-architect
---------------------------------------	---	---

[Users](#) | [Permissions](#) | [Access advisor](#)

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Simulate](#)[Remove](#)[Add permissions](#) ▼

🔍 *Filter policies by property or policy name and press enter*

< 1 > ⚙️

<input type="checkbox"/>	Policy Name ↗	Type	Description
<input type="checkbox"/>	+ AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.

[Users](#) > [Priya](#)

Summary

[Delete user](#)

User ARN	arn:aws:iam::543509858019:user/Priya ↗
Path	/
Creation time	2021-08-02 00:12 UTC+0530

[Permissions](#) | [Groups \(1\)](#) | [Tags](#) | [Security credentials](#) | [Access Advisor](#)

Sign-in credentials

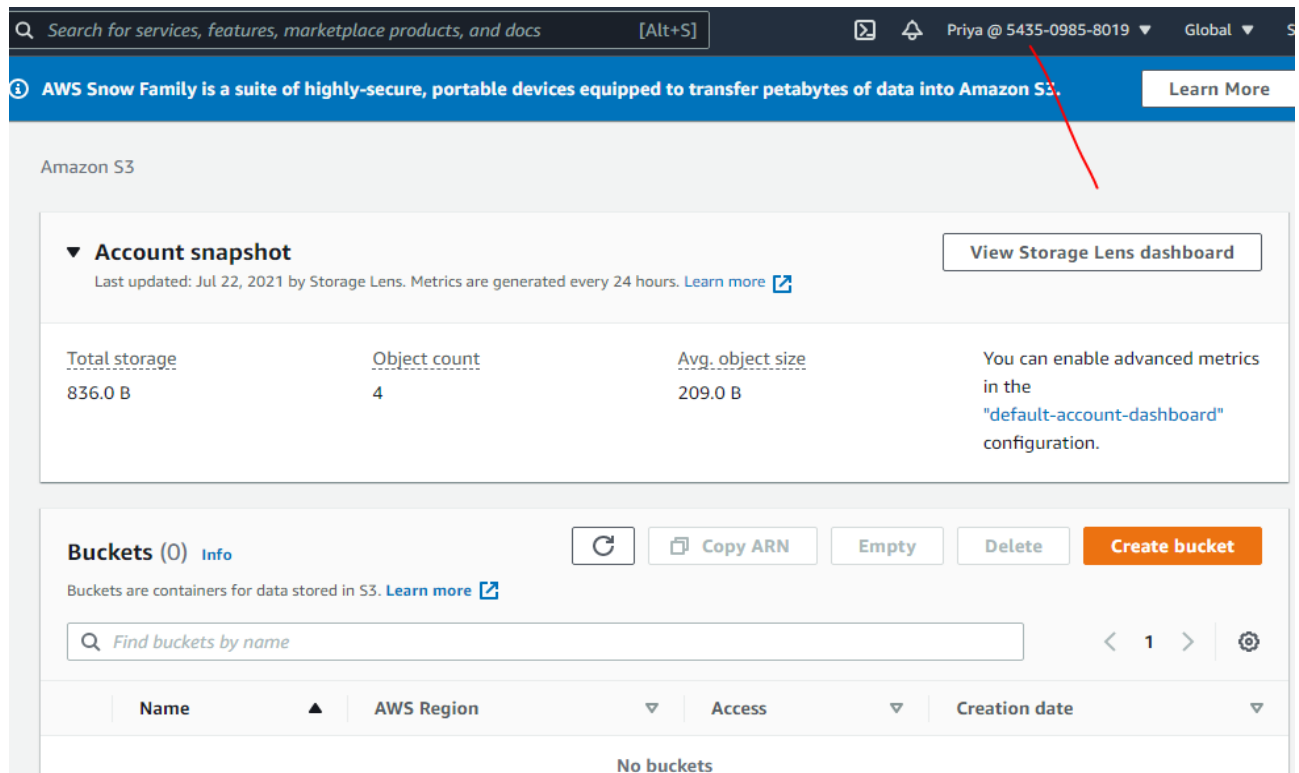
Summary • Console sign-in link: <https://543509858019.signin.aws.amazon.com/console> [↗](#)

Console password	Enabled (never signed in) Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None ✎

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

Here the group solution architect in which user priya having permission to S3 domain.



Here the group solution architect in which user priya is not having permission to Route53 domain.

